

Kiberfenyegetettség elemzés a NATO tagállamokat érintő geopolitikai eszkalációval összefüggésben

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NBSZ-NKI) a balti államokat érintő geopolitikai eszkalációval összefüggésben kiberfenyegetettségi elemzést készített az orosz állami, katonai és államhoz köthető kiberbűnözői tevékenységekről. Az elemzés bemutatja az aktuális geopolitikai helyzetet, a legismertebb támadói csoportok jellemző technikáit, valamint az NBSZ-NKI által javasolt védekezési intézkedéseket.

A Kreml 2026 májusának végén válaszlépések alkalmazását helyezte kilátásba, miután azzal vádolta Ukrainát, hogy Lettország légtérét és területét dróntámadások előkészítésére vagy indítására használja. Egy nappal korábban orosz hírszerzési források azt állították, hogy Lettország NATO-tagsága nem nyújt védelmet egy esetleges orosz megtorlással szemben. Az ilyen típusú politikai-katonai eszkaláció növeli annak kockázatát, hogy orosz állami vagy államhoz köthető szereplők kibereszközökkel is nyomást gyakoroljanak a balti államokra, illetve a NATO- és EU-tagállamok közös katonai és gazdasági övezetéhez kapcsolódó szervezetekre.

A támadók célja nem feltétlenül az azonnali, jelentős mértékű károk előidézése, hanem hozzáférések kiépítése, szolgáltatások zavarása, a reagálási képességek felmérése, hírszerzési előny szerzése, valamint a közbizalom gyengítése lehet.

Kiberfenyegetési szempontból kiemelt kockázatot jelentenek az orosz állami vagy államhoz köthető szereplők – különösen a Turla, az APT28 és az APT29 –, mivel korábbi európai tevékenységük alapján képesek célzott hozzáférésszerzésre, hírszerzésre és hosszabb távon aktiválható műveleti jelenlét kialakítására. A kockázat elsősorban azoknál a szervezeteknél jelentkezik, amelyek internet felől elérhető tűzfalakat, VPN-eket, e-mail szolgáltatásokat, webmail-felületeket, webportálokat, identitáskezelő rendszereket, peremeszközöket (edge device) vagy távoli adminisztrációs megoldásokat üzemeltetnek.

Ügyfeleinknek ezért javasolt kiemelt figyelmet fordítaniuk az internet felől elérhető rendszerek, a privilegizált hozzáférések, a beszállítói kapcsolatok felülvizsgálatára, valamint az elosztott szolgáltatás-megtagadásos támadások (DDoS) elleni ellenálló képesség kialakítására.

Támadási minta elemzés

A MITRE ATT&CK elemzés alapján az orosz állami háttérű vagy ahhoz kapcsolódó szereplők – kiváltképp a Turla, az APT28 és az APT29 – műveleteiben visszatérő mintázatként jelenik meg az internet felől elérhető rendszerek kompromittálása (T1190), a célzott adathalászat (T1566), a hitelesítő adatok megszerzésére irányuló jelszó-próbálgatásos támadások (T1110), valamint a kompromittált rendszereken végzett credential dumping (T1003), valamint legitim fiókokkal történő hozzáférésszerzés (T1078), külső távoli szolgáltatásokon keresztüli bejutás és perzisztencia (T1133), valamint fiókok manipulálásával történő tartós jelenlét kiépítése (T1098). A támadók gyakran alkalmaznak hamis bejelentkezési felületeket, ellopott vagy

TLP: CLEAR

Szabadon terjeszthető!

újrahasznosított hitelesítő adatokat, illetve privilegizált beszállítói hozzáférésekkel való visszaélést.

A csoportok jellemzően PowerShell, script és parancsértelmező-alapú végrehajtást alkalmaznak (T1059), majd rejtett, proxyzott vagy tunneling alapú kommunikációs csatornákon keresztül tartják fenn a kapcsolatot a kompromittált infrastruktúrával (T1071, T1090, T1105). Gyakori elem továbbá a rendszerszintű felderítés: fájlok és könyvtárak (T1083), futó folyamatok (T1057), valamint jogosultsági csoportok feltérképezése (T1069), az oldalirányú mozgás távoli szolgáltatásokon keresztül (T1021), valamint az adatok archiválása és fokozatos kiszivárogtatása (T1560, T1048, T1567). A műveletek során kiemelt szerepet kapnak a védelemkijátszási technikák, például folyamatmaszkolás, nyomeltüntetés és legitim adminisztrációs eszközök használata (T1036, T1070, T1218).

Az elemzett minták alapján a támadók elsődleges célja nem feltétlenül az azonnali károkozás, hanem a hosszú távú, rejtett hozzáférés fenntartása, az információszerzés, valamint szükség esetén zsarolási, reputációs vagy befolyásolási célú műveletek támogatása. Ezzel párhuzamosan továbbra is számolni kell DDoS-jellegű túlterheléses támadásokkal, hack-and-leak műveletekkel, illetve ransomware vagy adatlopással kombinált zsarolási kísérletekkel is, különösen olyan szervezetek esetében, amelyek nyilvános szolgáltatásokat, kritikus infrastruktúrát vagy nagy mennyiségű érzékeny adatot kezelnek.

A fenti MITRE ATT&CK minták és a jelenlegi geopolitikai környezet alapján megnövekedett kockázattal kell számolni különösen az alábbi kibertevékenységek esetében:

- hitelesítőadat-lopás és célzott adathalászat;
- hamisított belépési oldalak használata, különösen webmail, VPN és felhős szolgáltatások esetén;
- internet felől elérhető tűzfalak, VPN-ek, e-mail rendszerek, webportálok és peremeszközök (edge device) kompromittálása;
- perzisztens hozzáférések kiépítése;
- tunneling és rejtett távoli hozzáférési csatornák használata;
- privilegizált vagy beszállítói fiókokkal való visszaélés;
- DDoS- és hacktivista jellegű túlterheléses támadások;
- ransomware vagy adatlopással kombinált zsarolási kísérletek;
- hack-and-leak műveletek, kiszivárogtatás, reputációs támadás;
- kiberműveletek összehangolása befolyásolási vagy fizikai incidensekkel.

TLP: CLEAR

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Stealth	Defense Impairment	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
T1595: Active Scanning	T1583: Acquire Infrastructure	T1189: Drive-by Compromise	T1651: Cloud Administration Command	T1098: Account Manipulation	T1548: Abuse Elevation Control Mechanism	T1334: Access Token Manipulation	T1686: Disable or Modify System Firewall	T1557: Adversary-in-the-Middle	T1087: Account Discovery	T1210: Exploitation of Remote Services	T1577: Adversary-in-the-Middle	T1071: Application Layer Protocol	T1030: Data Transfer Size Limits	T1561: Disk Wipe
T1595.002: Vulnerability Scanning	T1583.001: Domains	T1190: Exploit Public-Facing Application	T1059: Command and Scripting Interactions	T1098.001: Additional Cloud Credentials	T1548.002: Bypass User Account Control	T1134.002: Create Process with Token	T1686.003: Windows Host Firewall	T1557.004: Evil Twin	T1087.004: Cloud Account	T1570: Lateral Tool Transfer	T1071.002: Mail Protocols	T1048.002: Exfiltration Over Alternative Protocol	T1561.001: Disk Content Wipe	
T1589: Gather Victim Identity Information	T1583.003: Virtual Private Server	T1133: External Remote Services	T1059.009: Cloud API	T1098.003: Additional Cloud Roles	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft	T1685: Disable or Modify Tools	T1110: Brute Force	T1087.002: Domain Account	T1021: Remote Services	T1560: Archive Collected Data	T1071.001: Web Protocols	T1048.002: Exfiltration Over Asymmetric-Encrypted Channel	T1498: Network Denial of Service
T1589.001: Credentials	T1584.006: Phishing	T1566: Phishing	T1059.007: JavaScript	T1098.002: Additional Email Delegate Permissions	T1134.002: Create Process with Token	T1140: Desubfuscate/Decode Files or Information	T1685.005: Clear Windows Event Logs	T1110.001: Password Guessing	T1087.001: Local Account	T1021.001: Cloud Services	T1560.001: Archive via Utility	T1092: Communication Through Removable Media	T1567: Exfiltration Over Web Service	
T1591: Gather Victim Org Information	T1596: Compromise Accounts	T1566.001: Spearphishing Attachment	T1059.001: PowerShell	T1098.005: Device Registration	T1134.001: Token Impersonation/Theft	T1006: Direct Volume Access	T1685.002: Disable or Modify Cloud Log	T1110.003: Password Spraying	T1482: Domain Trust Discovery	T1021.002: Remote Desktop Protocol	T1119: Automated Desktop Protocol	T1001: Data Obfuscation	T1567.002: Exfiltration to Cloud Storage	
T1598: Phishing for Information	T1586.003: Cloud Accounts	T1566.002: Spearphishing Link	T1059.006: Python	T1347: Boot or Logon Autostart Execution	T1098: Account Manipulation	T1211: Exploitation for Stealth	T1685.001: Disable or Modify Windows Event Log	T1555: Credentials from Password Stores	T1083: File and Directory Discovery	T1021.002: Remote Desktop Protocol	T1123: Information from Information Repositories	T1001.001: Junk Data		
T1598.003: Spearphishing Link	T1586.002: Email Accounts	T1566.003: Spearphishing via Service	T1059.005: Visual Basic	T1547.001: Registry Run Keys Startup Folder	T1098.003: Additional Cloud Credentials	T1564: Web Artifacts	T1484: Domain or Tenant Policy Modification	T1555.002: Credentials from Web Browsers	T1616: Group Policy Discovery	T1021.006: Windows Remote Management	T1213.003: Code Repositories	T1001.002: Steganography		
T1596: Search Open Technical Databases	T1584: Compromise Infrastructure	T1091: Replication Through Removable Media	T1059.003: Windows Command Shell	T1547.004: Winlogon Helper DLL	T1098.002: Additional Email Delegate Permissions	T1564.012: File/Path Exclusions	T1356: Modify Authentication Process	T1555.003: Credentials from Credential Manager	T1680: Local Storage Discovery	T1091: Replication Through Removable Media	T1213.006: Sharpoint	T1568: Dynamic Resolution		
	T1584.001: Domains	T1195: Supply Chain Compromise	T1203: Exploitation for Client Execution	T1037: Boot or Logon Initialization Scripts	T1098.005: Device Registration	T1564.001: Hidden Files and Directories	T1356.007: Hybrid Identity	T1606: Forge Web Credentials	T1040: Network Sniffing	T1550: Use Alternate Authentication Material	T1213.002: Encrypted Channel	T1573: Symmetric Cryptography		
	T1584.008: Network Devices	T1195.002: Compromise Software Supply Chain	T1199: Inter-Process Communication	T1037.001: Logon Script (Windows)	T1098.002: Additional Email Delegate Permissions	T1564.002: Hidden Window	T1556.007: Hybrid Identity	T1606.002: SAML Tokens	T1201: Password Policy Discovery	T1550.001: Application Access Token	T1005: Data from Local System	T1573.001: Symmetric Cryptography		
	T1584.004: Server	T1199: Trusted Relationship	T1159: Dynamic Data Exchange	T1037.004: RC Scripts	T1547: Boot or Logon Autostart Execution	T1070: Indicator Removal	T1112: Modify Registry	T1606.001: Web Cookies	T1120: Peripheral Device Discovery	T1550.002: Pass the Hash	T1039: Data from Network Shared Drive	T1665: Hide Infrastructure		
	T1584.003: Virtual Private Server	T1078: Valid Accounts	T1106: Native API	T1547.001: Registry Run Keys Startup Folder	T1098.002: Additional Email Delegate Permissions	T1070.008: Clear Mailbox Data	T1553.002: Code Signing	T1096: Input Capture	T1069: Permission Groups Discovery	T1550.003: Pass the Ticket	T1025: Data from Removable Media	T1105: Ingress Tool Transfer		
	T1584.006: Web Services	T1078.004: Cloud Accounts	T1053: Scheduled Task/Job	T1136.003: Cloud Account	T1547.004: Winlogon Helper DLL	T1070.004: File Deletion	T1553.006: Code Signing Policy Modification	T1553.002: Keylogging	T1069.001: Local Groups	T1069.002: Domain Groups	T1074.001: Local Data Staging	T1090: Proxy		
	T1587: Develop Capabilities	T1078.002: Domain Accounts	T1053.005: Scheduled Task	T1546: Event Triggered Execution	T1037: Boot or Logon Initialization Scripts	T1070.006: Timestamp	T1553.005: Code Signing Policy Modification	T1556.007: Hybrid Identity	T1556.007: Hybrid Identity	T1069.001: Local Groups	T1074.002: Remote Data Staging	T1090.002: External Proxy		
	T1587.003: Digital Certificates	T1078.003: Local Accounts	T1204: User Execution	T1546.008: Accessibility Features	T1037.001: Logon Script (Windows)	T1036: Masquerading	T1553.005: Mark-of-the-Web Bypass	T1556.007: Hybrid Identity	T1057: Process Discovery	T1074.002: Remote Data Staging	T1090.001: Internal Proxy			
	T1587.001: Malware	T1669: Wi-Fi Networks	T1204.002: Malicious File	T1546.015: Component Object Model Hijacking	T1037.004: RC Scripts	T1036.004: Masquerade Task or Service		T1040: Network Sniffing	T1012: Query Registry	T1114: Email Collection	T1090.003: Multi-hop Proxy			
	T1585: Establish Accounts		T1204.001: Malicious Link	T1546.013: PowerShell Profile	T1484: Domain or Tenant Policy Modification	T1036.005: Masquerade Resource Name or Location		T1012: Remote System Discovery	T1012: Remote System Discovery	T1114.002: Remote Email Collection				
	T1585.001: Social Media Accounts		T1047: Windows Management Instrumentation	T1546.003: Windows Management Instrumentation Event Subscription	T1484.002: Trust Modification	T1027: Obfuscated Files or Information		T1040: Network Sniffing	T1012: Query Registry	T1096: Input Capture	T1102: Web Service			
	T1588: Obtain Capabilities			T1133: External Remote Services	T1546: Event Triggered Execution	T1027.001: Binary Padding		T1003.006: DCsync	T1518.001: Security Software Discovery	T1056.001: Keylogging	T1102.002: Bidirectional Communication			
	T1588.007: Artificial Intelligence			T1556: Modify Authentication Process	T1546.008: Accessibility Features	T1027.010: Command and Scripting Interactions		T1003.004: LSA Secrets	T1082: System Information Discovery	T1056.002: Screen Capture				
	T1588.001: Malware			T1556.007: Hybrid Identity	T1546.015: Component Object Model Hijacking	T1027.013: Encrypted/Encoded File		T1003.001: LSASS Memory	T1016: System Network Configuration Discovery					
	T1588.002: Tool			T1112: Modify Registry	T1546.013: PowerShell Profile	T1027.011: Files Storage		T1003.003: NTDS	T1016.001: Internet Connection Discovery					
				T1137: Office Application Startup	T1546.003: Windows Management Instrumentation Event Subscription	T1027.006: DNS Smuggling		T1003.002: Security Account Manager	T1016.002: Wi-Fi Discovery					
				T1137.002: Office Test	T1068: Exploitation for Privilege Escalation	T1027.005: Indicator Removal from Tools		T1529: Steal Application Access Token	T1049: System Network Connections Discovery					
				T1542: Pre-OS Boot	T1055: Process Injection	T1027.002: Software Packing		T1649: Steal or Forge Authentication Certificates	T1007: System Service Discovery					
				T1542.003: Bootkit	T1055.001: Dynamic-link Library Injection	T1027.003: Steganography		T1558: Steal or Forge Kerberos Tickets	T1124: System Time Discovery					
				T1053: Scheduled Task/Job	T1053: Scheduled Task	T1542: Pre-OS Boot		T1558.003: Kerberoasting						
				T1053.005: Scheduled Task	T1078: Valid Accounts	T1055: Process Injection		T1539: Steal Web Session Cookie						
				T1595: Gather Victim Org Information	T1078: Valid Accounts	T1055.001: Dynamic-link Library Injection		T1552: Unsecured Credentials						
				T1078: Valid Accounts	T1078.004: Cloud Accounts	T1014: Rootkit		T1552.004: Private Keys						
				T1078.004: Cloud Accounts	T1078.002: Domain Accounts	T1684: Social Engineering								
				T1078.002: Domain Accounts	T1078.003: Local Accounts	T1684.001: Impersonation								
				T1078.003: Local Accounts		T1218: System Binary Proxy Execution								
						T1218.005: Mshta								
						T1218.011: Rundll32								
						T1221: Template Injection								
						T1078: Valid Accounts								
						T1078.004: Cloud Accounts								
						T1078.002: Domain Accounts								
						T1078.003: Local Accounts								

1. ábra: A három csoport (Turla, APT28, APT29) támadási technikai aggregált formában láthatók: a sötétebb szín magasabb előfordulási gyakoriságot vagy több csoport általi alkalmazást jelez. Forrás: MITRE ATT&CK® Navigator

Ajánlott intézkedések

Az NBSZ-NKI a fenyegetettséggel összefüggésben az alábbi intézkedések megtételét javasolja. Általánosságban elmondható, hogy az itt felsoroltak alkalmazása érdemben tudja javítani a szervezetek kibertámadások elleni rezisztenciáját.

MFA kötelező alkalmazása

A szervezetek haladéktalanul vezessenek be, vagy tegyenek kötelezővé többfaktoros hitelesítést minden kritikus hozzáférésnél.

Kiemelten érintett hozzáférések:

- adminisztrátori fiókok;
- VPN- és távoli hozzáférések;
- e-mail és webmail rendszerek;
- felhős adminfelületek;
- identitáskezelő rendszerek;
- privilegizált hozzáférések;
- beszállítói és karbantartói hozzáférések.

A hagyományos SMS- vagy push-alapú MFA önmagában nem tekinthető elegendőnek magas kockázatú hozzáférések esetén. Ahol lehetséges, FIDO2/WebAuthn, hardverkulcsos vagy más phishing-rezisztens megoldás alkalmazása javasolt.

Internet felől elérhető rendszerek azonnali felülvizsgálata és kitettségcsökkentése

A szervezetek készítsenek leltárt minden internet felől elérhető szolgáltatásról, és csökkentsék a szükségtelen kitettséget.

Kiemelten vizsgálandó rendszerek:

- tűzfalak;
- VPN-ek;
- e-mail gatewayek;
- webmail / OWA felületek;
- publikus webportálok;
- távoli adminisztrációs felületek;
- identitás- és hozzáféréskezelő portálok;
- peremeszközök (edge device);
- felhős menedzsmentkonzolok;
- fájlmegosztó és collaboration rendszerek.

Ajánlott intézkedések:

- nem használt szolgáltatások letiltása;
- adminisztrátori felületek internetes elérésének megszüntetése;
- hozzáférés korlátozása IP-cím vagy megbízható hálózat alapján;
- adminisztrátori portálok VPN, zero-trust vagy más védett hozzáférési réteg mögé helyezése;

- elavult vagy nem támogatott rendszerek kiváltása;
- külső támadási felület rendszeres ellenőrzése.

Fenyegetésvezérelt sérülékenységkezelés

A szervezetek javítsák a gyakran kihasznált, különösen internet felől elérhető rendszereket érintő sérülékenységeket.

Priorizálni szükséges az alábbi rendszereket:

- VPN és távoli hozzáférési megoldások;
- tűzfalak és edge security appliance-ek;
- e-mail és webmail rendszerek;
- webes portálok;
- identitáskezelő rendszerek;
- virtualizációs és felhős menedzsmentplatformok;
- fájlmegosztó és együttműködési szolgáltatások.

A havi vagy rutinszerű patch-ciklus önmagában nem elegendő. A magas kockázatú, aktívan kihasznált vagy széles körben célzott sérülékenységeket gyorsított eljárásban kell kezelni. Az NBSZ-NKI rendszeresen tesz közzé weboldalán sebezhetőségi információkat, melyeket javasolt napi szinten követni.

Feltételes és kockázatalapú hozzáférés bevezetése

A hozzáféréseket kockázatalapú szabályokkal szükséges védeni. Nem elegendő a felhasználónév, jelszó és MFA kombinációjára hagyatkozni.

Ajánlott kontrollok:

- magas kockázatú országokból érkező belépések blokkolása vagy külön ellenőrzése;
- TOR, anonimizáló VPN, proxy és adatközponti IP-k szigorú kezelése;
- új eszközről vagy szokatlan helyről történő belépés újrathitelesítése;
- adminisztrátori felületek elérése csak jóváhagyott eszközről és hálózatról;
- privilegizált műveletekhez dinamikusan megjelenő kiegészítő hitelesítés (step-up authentication);
- feltételes hozzáférési szabályok rendszeres felülvizsgálata.

Privilegizált hozzáférések szegmentálása és szigorítása

A kiemelt jogosultságokat javasolt minimálisra csökkenteni, külön kezelni és folyamatosan monitorozni.

Ajánlott intézkedések:

- napi használatú fiókok és adminisztrátori fiókok szétválasztása;
- domain admin és global admin jogok minimalizálása;
- Just-in-Time és Just-Enough-Administration alkalmazása;
- külön adminisztrátori fiókok használata kritikus rendszerekhez;
- privilegizált munkamenetek naplózása;
- adminisztrátori tevékenység riasztásalapú monitorozása;
- inaktív vagy indokolatlan adminisztrátori jogok visszavonása;
- beszállítói adminisztrátori jogok időbeli és funkcionális korlátozása.

Perzisztens hozzáférések, tunneling és anomáliák keresése

A szervezetek auditálják rendszereiket olyan hozzáférések azonosítását keresve, amelyeket későbbi hírszerzési vagy zavaró műveletekhez használhatnak fel.

Keresendő minták:

- ismeretlen vagy ritkán használt távoli kapcsolatok;
- szokatlan tunneling forgalom;
- nem dokumentált VPN- vagy proxykapcsolatok;
- hosszú életű, alacsony zajszintű hálózati kapcsolatok;
- szokatlan outbound forgalom kritikus rendszerekről;
- peremeszközök (edge device) konfigurációmódosítások;
- újonnan létrehozott adminfiókok;
- nem jóváhagyott remote management eszközök;
- naplózás leállítása, törlése vagy csökkentése;
- szokatlan szolgáltatásfiók-használat.

Távoli menedzsment aktivitás fokozott monitorozása

A távoli adminisztrációs tevékenységeket külön kockázati kategóriaként indokolt kezelni, ezen belül az alábbiakra szükséges figyelmet fordítani:

- szokatlan RDP, SSH, VPN vagy adminisztrátori portál-belépésekre;
- munkaidőn kívüli adminisztrátori tevékenységekre;
- tömeges konfigurációmódosításokra;
- új távoli menedzsment eszközök telepítésére;
- szokatlan fájlmozgásokra;
- beszállítói fiókok rendellenes aktivitására;
- peremeszközök (edge device) beállításainak módosítására;
- távoli hozzáférési szolgáltatások degradációjára vagy manipulációjára.

DDoS-védelem megerősítése

A DDoS-támadások célja nem kizárólag a technikai rendelkezésre állás ellehetetlenítése lehet, hanem az intézmény megbízhatóságba vetett bizalom gyengítése is. Ezért a DDoS-védelmet üzletmenet-folytonossági és válságkommunikációs kérdésként is kezelni kell.

Ajánlott intézkedések:

- DDoS-mitigációs szolgáltató előzetes bevonása;
- CDN és forgalomszűrés alkalmazása;
- autoscaling biztosítása kritikus webes szolgáltatásoknál;
- upstream szolgáltatókkal előre egyeztetett eszkálició;
- alternatív kommunikációs csatornák kijelölése;
- szolgáltatáskimaradásra vonatkozó kommunikációs sablonok előkészítése;
- DDoS-gyakorlatok vagy technikai tesztek végrehajtása.

Beszállítói és harmadik feles hozzáférések felülvizsgálata

A kritikus beszállítók és szolgáltatók hozzáférései kiemelt kockázatot jelentenek. A szervezetek vizsgálják felül minden harmadik fél hozzáférését, különösen karbantartók, IT-outsourcing partnerek, védelmi beszállítók, logisztikai partnerek és közlekedési rendszereket támogató szolgáltatók esetén.

Elvárható minimumkövetelmények:

- MFA;
- naplózási követelmények teljesítése;
- privilegizált hozzáférések szegmentálása;
- távoli menedzsmenttevékenység monitorozása;
- incidensjelentési kötelezettség;
- hozzáférések rendszeres felülvizsgálata;
- ideiglenes hozzáférések automatikus lejáratása;
- hozzáférések azonnali visszavonása szerződés vagy feladat lezárásakor.

Naplózás, észlelés és riasztási szabályok megerősítése

A szervezetek vizsgálják meg és biztosítsák, hogy a kritikus rendszerek naplózása teljes, központilag gyűjtött és visszamenőlegesen vizsgálható legyen.

Kiemelten naplózandó események:

- sikeres és sikertelen bejelentkezések;
- privilegizált műveletek;
- adminisztrátori jogok kiosztása és visszavonása;
- MFA-módosítások;
- új fiókok létrehozása;
- szolgáltatásfiókok használata;
- VPN- és távoli hozzáférési események;
- konfigurációmódosítások;
- naplózás kikapcsolása vagy módosítása;
- adatletöltési és tömeges fájlmozgási események.

A naplót védeni szükséges törlés, módosítás és jogosulatlan hozzáférés ellen.

Incidens és befolyásolási művelet együttes kezelése

Egy incidens reputációs vagy akár információs művelettel is párosulhat, ezért incidens esetén nem elegendő kizárólag technikai vizsgálatot indítani.

Párhuzamosan vizsgálandó:

- adatlopás vagy kiszivárogtatás lehetősége;
- hack-and-leak narratívák megjelenése;
- hamisított dokumentumok terjedése;
- közösségi médiás dezinformáció;
- célzott reputációs támadás;
- vezetők, alkalmazottak vagy beszállítók doxolása;

- DDoS- és propagandaaktivitás egyidejű megjelenése.

A kiberbiztonsági, kommunikációs, jogi, adatvédelmi, valamint vezetői válságkezelési folyamatokat ajánlott egységesen kezelni.

NBSZ-NKI CSIRT koordináció előkészítése

A szervezetek számára javasolt előzetesen meghatározni, hogy incidens esetén kivel, milyen kommunikációs csatornán, valamint milyen döntéshozatali rend szerint történik a kapcsolatfelvétel.

Előkészítendő:

- NBSZ-NKI CSIRT-kapcsolat;
- internetszolgáltatói eskaláció;
- felhőszolgáltatói eskaláció;
- DDoS-mitigációs szolgáltató kapcsolata;
- jogi és adatvédelmi kapcsolattartók;
- kommunikációs és sajtókapcsolati felelősök;
- vezetői döntéshozói ügyeleti rend.

Az eskalációs listákat naprakészen kell tartani és rendszeresen tesztelni kell.

Üzletmenet-folytonossági és helyreállítási képességek tesztelése

A szervezetek ne csak dokumentálják, hanem gyakorolják is a kritikus szolgáltatások kiesésére vonatkozó eljárásokat.

Gyakorlandó incidenskezelési forgatókönyvek:

- e-mail nélküli működés;
- VPN-kiesés;
- DDoS alatti ügyfél- és lakossági kommunikáció;
- ransomware utáni helyreállítás;
- kritikus rendszerek izolálása;
- kézi vagy alternatív üzemeltetési mód;
- mentésekből történő visszaállítás;
- hatósági bejelentési folyamat;
- nyilvános kommunikáció reputációs támadás esetén.

A mentéseket rendszeresen tesztelni szükséges, a mentési környezetet pedig el kell különíteni az éles rendszerektől, és védeni kell a jogosulatlan módosítással vagy törléssel szemben.

Fenyegetettségi információk követése és szervezetspecifikus támogatás

A szervezetek számára javasolt a releváns fenyegetettségi információk folyamatos nyomon követése, különös tekintettel a kritikus infrastruktúrákat, valamint a kormányzati, közlekedési, logisztikai, energetikai, pénzügyi és telekommunikációs szektorokat érintő biztonsági eseményekre és incidensekre.

Az NBSZ NKI javasolja, hogy az érintett szervezetek rendszeresen kövessék az NBSZ-NKI weboldalán közzétett riasztásokat, tájékoztatókat és fenyegetettségi információkat, valamint használják fel a havi CTI elemzésekben szereplő megállapításokat saját védelmi intézkedéseik, detektálási szabályaik és kockázatértékelésük aktualizálásához.



TLP: CLEAR

Szabadon terjeszthető!

A jogosult, kritikus infrastruktúrát üzemeltető szervezetek soron kívüli, szervezetspecifikus fenyegettségelemzést kérhetnek az NBSZ-NKI-tól a cyberthreat@nki.gov.hu e-mail címen.

Nemzetbiztonsági Szakszolgálat
Nemzeti Kiberbiztonsági Intézet
Telefon: +36-1-336-4833

TLP: CLEAR